CSC-EPL-87/001

(2)

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF SECURITY DYNAMICS ACCESS CONTROL ENCRYPTION SYSTEM

31 March 1987

Distribution
Inside Front Cover

Approved for public release;
distribution unlimited

SUB-SYSTEM EVALUATION REPORT

SECURITY DYNAMICS, INC.

ACCESS CONTROL ENCRYPTION SYSTEM

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

March 31, 1987

CSC-EPL-87/001
Library No. S228,455

FOREWORD

This publication, the Sub-system Evaluation Report, Security Dynamics, Inc., Access Control Encryption system, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the evaluation of Security Dynamics' Access Control Encryption (ACE)(1) system. The requirements stated in this report are taken from DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, dated December 1985.

Approved:

March 31, 1987

Eliot Sohmer
Chief, Product Evaluations and Technical Guideline,
National Computer Security Center

[1] ACE is a registered trademark of Security Dynamics, Inc.

ACKNOWLEDGEMENTS

Evaluation Team Members

James L. Arnold

Thomas A. Ambrosi

William B. Geer

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

CONTENTS

EXECUTIVE SUMMARY

The Access Control Encryption (ACE) system has been evaluated by the National Computer Security Center (NCSC). ACE is considered to be a security sub-system rather than a complete trusted computer system, therefore it was evaluated against a relevant subset of the requirements from the DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (Criteria). This subset includes identification & authentication (I & A) and audit. Additionally, ACE implements a technology to reliably verify an authenticated connection.

The NCSC evaluation team has determined that ACE is capable of applying these security features to any system that uses standard communication channels. ACE maintains user I & A by requiring each user to enter a proper passcode prior to granting access to the host system or, in the case of an ACE administrator, to the ACE system maintenance menus. The authenticated connection, achieved by requiring the Access Control Module (ACM) to authenticate itself to the user, provides some assurance to users that they are responding to ACE and not to a personal identification number spoofing program. Audit records can be created for virtually everything associated with the ACM, including attempted connections to the host and any ACE system maintenance that occurs.

These security mechanisms can be maintained only if the ACM, a stand-alone integrated hardware/software device, can be protected from physical tampering. Additionally, the system must also be configured such that the ACM cannot be bypassed (i.e., by unprotected communication channels).

[illegible] — Computer security; encryption, [illegible],
[illegible] evaluation; (KT) ←

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems; that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Introduction

Sub-systems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub-system evaluation is limited to consideration of the sub-system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub-system's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

The Access Control Encryption (ACE) system is an integrated hardware/software package which provides user identification & authentication and authenticated connection mechanisms for a host system. In addition, it audits all ACE mediated access attempts to the host. The ACE system is composed of two components, the Access Control Module (ACM) and the SecurID card. The ACM is a stand-alone device which, when installed with standard RS-232 or RS-422 communication lines, will ask users to identify and authenticate themselves before it will allow a connection to be established to the host. Each ACM has the capability to mediate multiple communication channels. The number of potential channels, varying from 8 to 128, is dependent upon the model of the ACM used. The ACM can also be configured such that it authenticates itself to the user before asking the user to give authentication data, thereby providing an authenticated connection. The SecurID card generates a series of pseudo random numbers (PRN). One such PRN is always displayed in a liquid crystal display on the face of the SecurID card, and is used by the user, in addition to a personal identification number (PIN), to identify himself to the ACM.

Evaluation of Functionality

Identification & Authentication

Before gaining a connection to the host computer, each user must enter a valid PIN and PRN. These values serve to identify and authenticate the user to the ACM, and implicitly authenticate the user to the host machine. The PIN/PRN combination can be entered one of two ways, determined by the initial system configuration. The first method is to enter the PIN followed immediately by the PRN. This may present a security problem if the PIN is transmitted in the clear. However, the same problem is inherent in most standard password mechanisms and is no more severe in this case. The other method involves adding the PIN to the PRN without carry. This method effectively hides the PIN, because the constant PIN is being added to a seemingly arbitrary number creating what appears to be an equally arbitrary number.

Product Evaluation

Each SecurID card has a serial number and at least one PIN which are unique to any given ACE system. It can be changed only by the ACE administrator, who executes an appropriate function to generate a new PIN. The PINs can only be randomly generated by the ACM, and cannot be set manually. To obtain the newly generated PIN, the card holder must enter the card's serial number and current PRN at a standard passcode prompt, after which the new PIN will be displayed on the terminal for approximately ten seconds. PIN data cannot be retrieved from the ACM, even by an ACE administrator.

The PRNs generated by the SecurID cards are seemingly random. The card's PRN generating algorithm is synchronized with a similar algorithm in the ACM. At predetermined intervals of time, determined by the purchased configuration, the PRN changes. Any variations in the two clocks involved are handled by a proprietary method which seems to work very well.

At ACE system generation time, each card can be programmed to self-destruct after a predetermined period of time. Destruction consists of the card erasing all of its memory, rendering itself useless. It can then never be reinitialized or reused for its original purpose. The administrator can also enable and disable individual cards for access, at the ACM.

Access to the ACM while under duress can be detected by the ACE system. This is accomplished through the use of a duress PIN. This alternate PIN seems to function exactly as the standard PIN would, except the system realizes that the user is under duress and can send out the appropriate alarms.

The system can also detect some forms of unauthorized access attempts. Repeated attempts, the count of which is ACE administrator settable, to enter an invalid PIN and a valid PRN result in the card associated with the given PRN being locked out of the system, the presumption being that the card has been lost or stolen and is in unauthorized possession. Repeated attempts to enter a valid PIN and an invalid PRN results in, after a valid PIN and PRN are entered, the user being asked for the next PRN. This is to ensure that an unauthorized individual has not successfully guessed a correct PRN once.

Audit

The ACE system provides comprehensive audit capabilities for all accesses to the ACM. The audit data can be broken down into incident, exception, :and activity reports. The incident report is concerned with anything that denies the user a connection to the host (e.g., bad PIN, bad PRN, generating a new PIN, etc.). The exception report is concerned with anything exceptional that might occur to the system (e.g., PIN change, failure to connect to host, user data changes, etc.). The activity report contains information pertaining to virtually any form of activity related to the ACM, including failed connections, successful connections, ACM menu usage, terminated logons, etc.

The audit records can be viewed only by an ACE system administrator. He can print them in various formats either on a terminal or a printer. In addition, not all of the records need be viewed; they can be selected by user, port, or time. They can also be transferred to another computer system via one of the ACM terminal ports.

The audit information is stored in Random Access Memory in the ACM and is protected by battery backup. About 1000 records before the storage area is filled, a warning message occurs every time an administrator logs on. If the message is ignored and the audit storage area is exhausted, the system begins to lose audit data. After such an occurrence, each administrator is given a warning message indicating the problem each time he logs on.

Authenticated Connection

The ACE system can be configured such that, before asking the user for a valid PIN and PRN, it asks the user for his SecurID card serial number. After a valid serial number is entered, the ACM will display the pseudo-random number that is currently on the SecurID card, after which access may be gained through the use of any following PRN. This mechanism gives the user some assurance that he is communicating with the correct ACE system, as opposed to a spoofing program or something similar.

Evaluation of Documentation

The ACE system documentation package consists of one document, the ACE System Manual, 1986, 16 Port Hardware Version. The ACE System Manual is a compendium of a preface and two specific user guides, the ACE System User's Guide and the ACE System Administrator's Guide. These documents, which are described below, provide a detailed description of the security features offered by the ACE system. The documentation was found to be complete and accurate, except as noted later in this report.

Preface

The Preface is a single page overview of the ACE System Manual. It describes the breakdown of the manual into sections, and briefly what each section contains.

ACE System User's Guide

This eight-page document is intended for use by end users and administrators. It contains a general introduction to the ACE system, as well as detailed instructions for its overall use.

I. Introduction

The introduction presents a brief overview of the ACE system's configuration and use.

II. Logging On

This section describes how to use the SecurID card and the ACM to logon to the ACE system and gain a connection to the host. It provides a step-by-step explanation of the logon procedure. Examples of both correct and incorrect logon procedures are given, as well as how to recover from invalid logon attempts.

For this evaluation, Security Dynamics provided an addendum which describes all modes of logon. For normal use, only the logon modes in the purchased configuration would be described.

III. The SecurID Card

This section provides information specific to the SecurID card and some guidelines for its care.

ACE System Administrator's Guide

This document includes an Installation Guide, a Software Manual, ar^d Hardware Specifications.

Installation Guide

This seven-page document is intended for the individual installing the ACE system. It provides detailed installation instructions.

I. Introduction

The introduction describes the elements that make up the ACE system hardware, and provides a brief explanation of their installation procedures.

II. Installation

The installation section provides detailed information about unpacking, locating, powering, connecting, and activating the ACM. It contains a list of the items delivered, as well as diagrams of the ACM to facilitate the installation process. This section also describes the procedure to access the administrative menus.

Software Manual

This eighty-three-page document is intended for the individuals who will be administrating the ACE system. It provides a description of the ACE system functions and an introduction for new ACE administrators.

Preface

The preface presents an overview of the following chapters.

Chapter I. The ACM Menus

This chapter provides an overview of the ACE system menu structure. It introduces important concepts that are necessary in understanding the entire system.

Chapter II. System Administration

This chapter provides an overview of the responsibilities of the system administrator. It also explains the administrative menu and functions of the ACE system.

Chapter III. Report Generation

This chapter discusses the audit report generation process.

Chapter IV. Changing User Records

This chapter explains how user records can be maintained and edited.

Chapter V. The ACM System Memory Structure

This chapter provides details concerning the system's memory allocation and usage.

Chapter VI. Port Parameters

This chapter explains how the ports can be configured to match the requirements of the host system and terminals.

Chapter VII. System Parameters

This chapter discusses the set of variables that affect the overall system operation.

Appendices

A. Quick-Reference Guide to Operations

This appendix provides a quick-reference guide for many frequently used operations.

B. Complete ACE Menu Listings

This appendix displays all of the ACE system menus.

C. Complete List of Log Record Types

This appendix provides a list of the different types of audit log records that are available in the ACE system.

Hardware Specifications

This three-page document provides the hardware specifications for the ACE system.

I. Physical/General Specifications

This section describes the physical and electrical characteristics and requirements, as well as the operating specifications, of the ACM.

II. I/O Hardware

This section describes general I/O characteristics and pin configurations.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The ACE system can be used, as-is from the manufacturer, to add security to virtually any computer system that uses standard communication protocols. The ACE system can be incorporated into dial-up communication lines, or into terminal-to-host connections that use RS-232 or RS-422 communication links. However, it is necessary that the data terminal ready (DTR) connections function properly. If DTR is held high, the ACE system will not disconnect. If held low, the system will not connect at all.

When installed as tested, the ACM will monitor all access attempts to the host. It will also maintain an audit log of all such attempts, with the exception of those audit records lost when the audit buffer overflows. The ACE system will add assurance that the user trying to connect to the host is a valid user. In addition, the system can be configured such that it is capable of authenticating itself to the user, assuring the user that he is communicating with the proper system.

The ACE system is independent of the host and cannot be tampered with by anyone who is using the host. The only individuals capable of altering the system are the ACE system administrators. These individuals are given special access cards that are recognized by the ACM at connection time.

The ACE system has some abilities, transparent to the user, to detect and lock out unauthorized users. The periodically changing PRNs that are part of the authorized passcode make it difficult to steal or borrow passwords, which are common problems with standard fixed-password systems. Even though the passcode is transmitted in the clear (i.e., not encrypted) there is no loss of security, because each passcode is valid only once.

The system can also implement a duress feature. When the duress feature is available to the given system configuration, each user is provided with an alternate duress PIN. If this PIN is used instead of the standard PIN at connection time, the ACE system recognizes that the user is connecting under duress and generates the appropriate alarms and messages. This occurrence is transparent to the user trying to connect. The alarms and associated messages can be sent, at the security administrator's option, to the host system or to whatever mechanisms have been installed for such an occurrence.

PRODUCT TESTING

Test Procedure

Testing represents a significant portion of a sub-system evaluation. The test suite used by the evaluation team tested ACE identification & authentication, authenticated connection, and audit functions. This functional test suite focused upon those security features identified in the Software Manual section of the ACE System Manual, 1986, 16 Port Hardware Version. The test suite consisted of five parts. The first tested that all functions available to the ACE administrator performed as documented. The second part involved an effort to overflow the audit data storage mechanism, in order to determine how the system would respond. The third part tested that the connection provided by the ACM was disabled properly as a result of a disconnect signal from a modem, causing data terminal ready to drop. The fourth part tested the functionality of the duress PIN feature. Finally, the fifth part of the test suite attempted to gain access to the host computer using the information provided by the authenticated connection mechanism.

All tests were performed using an ACM, 16 Port Hardware Version, connected between a terminal and host communicating with standard RS-232 protocol. Later during testing, the system was reconfigured to include a modem pair between the ACM and the host system. This allowed us to determine how the ACM would react to dial-up, as opposed to direct connect, communications.

Test Results

Menu Functional Tests

Extensive testing of all administrator functions produced positive results. With the following exceptions, every function available to our ACM model performed as stated in the ACE System Manual, 1986, 16 Port Hardware Version.

> The disable port option was improperly documented. However, the description is implied in the title.

Product Testing

The configuration mode enable option is not documented, except for a warning against its use. This flag is used for initial system generation and should not be used without the appropriate instructions from Security Dynamics.

Because of limitations on our test configuration, we were only able to determine that the system would not allow new cards to be added to the system once the maximum number were allotted. This maximum is fixed in the purchased configuration.

Audit Log Overflow Test

It was determined that about 1000 records before the audit storage area is filled, a warning message occurs every time an administrator logs on. If the warning message is ignored and the storage area is exhausted, an audit overflow warning message will occur every time an administrator logs on and all newly created audit records will be lost. This occurrence is transparent to all non-administrators.

Dial-up Communication Test

It was determined that dial-up connections to ACE function properly (i.e., the ACE system disconnected when either modem caused the data terminal ready signal to drop).

Duress PIN Test

It was determined that the duress PIN functioned as documented. Audit records are generated to indicate that an access under duress has occurred. While under duress, a user (including an administrator) has no access to information pertaining to that fact. Since the NCSC had no external duress alarm equipment of its own, this mechanism went untested.

Authenticated Connection Test

Numerous attempts to illegally connect using the PRNs provided by the authenticated connection mechanism were unsuccessful. Thus, the team believes that the data provided by this mechanism, although providing assurance to the user, cannot be used to authenticate that user. This is as it should be, and the feature performs as claimed; the authenticated connection is established and the host-provided code cannot be abused.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION / DOWNGRADING SCHEDULE

3. DISTRIBUTION / AVAILABILITY OF REPORT
Unclassified:
Distribution Unlimited

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
CSC-EPL-87/001

5. MONITORING ORGANIZATION REPORT NUMBER(S)
S 228,455

6a. NAME OF PERFORMING ORGANIZATION
National Computer Security Ctr

6b. OFFICE SYMBOL (If applicable)
C1

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS (City, State, and ZIP Code)
9800 Savage Rd
Fort George G. Meade, MD

7b. ADDRESS (City, State, and ZIP Code)

8a. NAME OF FUNDING / SPONSORING ORGANIZATION

8b. OFFICE SYMBOL (If applicable)

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS (City, State, and ZIP Code)

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11. TITLE (Include Security Classification)
(U) Final Evaluation Report, Security Dynamics' Access Control System

12. PERSONAL AUTHOR(S)
J. Arnold, T. Ambrosi, W. Geer

13a. TYPE OF REPORT
Final

13b. TIME COVERED
FROM ________ TO ______

14. DATE OF REPORT (Year, Month, Day)
870331

15. PAGE COUNT
22

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
NCSC TCSEC sub-system Security Dynamics Access Control Encryption System (ACE)

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The Security Dynamics Access Control Encryption System (ACE) was evaluated against the identification, authentication, and audit requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985. In addition, ACE was found to implement a technology which reliably verifies authenticated connections. The ACE system is designed to add assurance to existing trusted computer systems, and also to provide access controls to untrusted computer systems. This report documents the findings of the evaluation of this product.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
LTC Lloyd D. Gary, Jr.

22b. TELEPHONE (Include Area Code)
(301) 859-4458

22c. OFFICE SYMBOL
C/C12

Previous editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

☆U.S. Government Printing Office : 1987 - 721-851/60344